Exhibit O

Exhibit O-1

STANDARD PRACTICE GUIDE

THE UNIVERSITY OF MICHIGAN

NUMBER	601.11
DATE ISSUED:	12/1/93
PAGE	1 OF 6

NEW ISSUE

SECTION: General University Policies

SUBJECT: Privacy of Electronic Mail and Computer Files at the University of Michigan

Applies to: All Employees

I. Policy

At the University of Michigan, electronic mail and computer files are considered private to the fullest extent permitted by law. Ordinarily, access to electronic mail or computer files requires permission of the sender/recipients of a message or the owner of the file (the person to whom the account ID is assigned), court order, or other actions defined by law. In the event of a University investigation for alleged misconduct, e-mail or files may be locked or copied to prevent destruction and loss of information.

II. Policy Interpretations

The University of Michigan is a large, rich, and complex information technology environment. Different procedures for handling mail services are used at different sites across the institution. While it is not necessary that uniformity be achieved, it is desirable that there be coherence among the systems and in the way in which mail services are provided. In this way customers and service providers may be clear in their expectations regarding these services.

While the University's policy on proper use of information resources (Standard Practice Guide #601.7, "Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan") does not refer to electronic mail specifically, it characterizes as unethical and unacceptable any activity through which an individual:

- Interferes with the intended use of the information resources.
- Seeks to gain or gains unauthorized access to information resources.
- Without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

It is important to achieve clarity on several important points as the University community implements this policy.

1. What is the "intended use of the information resources"?

The Proper Use Policy makes reference to provision of information resources in order for the students, staff, and faculty to create intellectual products, collaborate, and communicate with colleagues. It also states that the University encourages access to knowledge and sharing of information in furtherance of the University's mission of instruction, research, and service. The information resources of the University are intended primarily for activities related to accessing, sharing, and creating information and collaborating with other members of this and other communities for scholarly and work-related communications. Secondarily, they are intended for use to enhance community.

2. Does the use of electronic mail and computer files exclusively for personal purposes fall within these guidelines?

Gilbert R Whitaker Jr

ISSUED BY
Provost and Executive Vice President for Academic Affairs

Open communication within a diverse institution such as this is critical to building a sense of community. Members of the community also strive for the most responsible use of the institutional resources. Therefore, limiting the number of purely personal electronic messages and files is appropriate and reasonable. Users at the University of Michigan are encouraged to use the communication resources primarily for purposes described in the preceding paragraph. Occasional and incidental social communications using electronic mail are not disallowed by this policy. However, each user should comply with specific policies of their individual units.

A unit manager concerned about an employee's potential violation of the University's Proper Use Policy (for example, excessive use of electronic mail for personal use or spending large quantities of time in electronic social conferencing) should NOT unilaterally seek to gain access to an employee's electronic communications. Instead, the manager should:

a) Review whether or not expectations and standards in this area have been well communicated and made clear to the employee.

b) Pursue direct communication with the employee regarding the issue.

c) Proceed as one would handle any personnel-related disciplinary action.

3. What is unauthorized access to information resources in this regard?

Generally, a good guideline to follow is that authors or parties to electronic mail should be the primary sources of authorization in granting access to their information or files. Third party access to electronic mail ordinarily may only be accomplished through either the sender or the recipient(s) of that mail.

4. Is it possible to invade the privacy of individuals . . . WITH authorization?

Since University resources are being used to create and store files, users should understand that the University must assign certain individuals responsibility for maintaining, repairing, and further developing those resources. In the normal course of doing their assigned work some individuals, by virtue of their positions within the University and their specific responsibilities, may have special access privileges to hardware and software and therefore to the content that resides in those resources. The University will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that such individuals are selected for their judgment and ethics, as well as their technical expertise. Such positions, and the individuals who hold them, will be governed through defined responsibilities and procedures. (See section III, "Standards for Postmasters," section IV, "Interpretive Guidelines and Procedures for System Administrators and and Computing Service Managers," below.)

5. How possible is it that electronic mail might be inadvertently seen?

Electronic mail may pass out of one machine environment, across a network, and into another totally different machine environment even within the University of Michigan campus. This transport becomes increasingly complicated as mail travels between universities, states, or nations. Each time the information technology hardware, software, and service environment changes, the level of security may be affected.

SECTION: General University Policies

SUBJECT: Privacy of Electronic Mail and Computer Files at the Univerisity of Michigan

In addition to differing security levels in different machine environments, electronic mail may also be compromised because of an individual's own difficulty in sending a message to an intended recipient. The sender may be uncertain about remote addressing; the message may not be deliverable, and a rejection message may be generated. If such rejections can be delivered to the original sender, ordinarily no person sees the message. If, however, the message can't be delivered to the original sender, systems can be configured to either pass the message to someone (a postmaster) for assistance or to discard the rejection without the sender knowing anything about the problem.

Postmasters are individuals who have the specific duties of enabling undeliverable mail to reach its destination, handling other delivery problems, and answering user questions about mail travel. Users should know that mail that is deliberately sent to postmasters for advice or mail that is undeliverable will be seen by others. Postmasters observe procedures and privacy standards analogous to those used by postmasters who receive letters in a post office.

6. How does the Michigan Freedom of Information Act (FOIA) affect the privacy of my electronic mail or computer files?

Federal and state laws ultimately determine whether or not there is a legal right to privacy of electronic mail, conferences, and computer files and the context of any such privacy rights. The University policy is that the Electronic Communications Privacy Act of 1986,(ECPA), state laws, and the expectations of the users require electronic mail, conferencing, file transmittal, and file storage to be kept private except as authorized by the owner, sender, or recipient of the information or as otherwise authorized by law. As yet, interpretations regarding the right to privacy are unsettled, the law is untested, and the interaction between ECPA, FOIA and privacy rights is unclear. Consequently, creators of electronic mail or computer files should be aware that it is possible that such mail or files may be disclosed to a third party without their consent because of a future court ruling.

7. What material may be retrievable if required by law?

Because systems on which users do their communications and computing vary widely, so too do back-up and save procedures. Users need to be informed about the back-up procedures in the environment in which they are working because those procedures will ultimately determine what information has been retained in the course of backing up the system and perhaps what may be accessible by others through legal means. For instance, within the MTS environment, a deleted or expired message will entirely disappear and be unretrievable after 28 days. (Senders may override the automatic expiration of messages by specifying longer parameters.) Messages that become part of a forwarding or history chain may be retrievable longer. Filesave procedures in each environment determine what material is saved and in what form.

8. What constitutes a record/document under FOIA?

FOIA requires the University to disclose "public records," which are defined as any writings prepared, used, owned, possessed, or retained by any part of the University of Michigan in the performance of its official function. "Writing" is broadly defined. FOIA does not require the University to create a record that does not already exist.

9. How does federal law affect the privacy of my e-mail or files?

The Electronic Communications Privacy Act of 1986 (ECPA) is the only existing federal law specifically governing e-mail. Under the ECPA there is privacy protection against both interception of electronic communications while in transmission and against unauthorized intrusion into e-mail stored on the system. Interception of electronic communication is prohibited (section 101-100 Stat 1850), and service providers of electronic communications cannot intentionally divulge communication contents, with certain exceptions (section 102). These provisions protect the privacy of electronic communications in general.

10. Are electronic mail and social conferencing materials considered official documents?

The question of whether electronic mail, social conferencing communication, or other electronic files are considered a "writing" under FOIA has not been addressed by this state's courts. There also has been no decision made on whether personal e-mail messages and social conferencing communications are prepared, used, owned, possessed, or retained by the University in the performance of its official function so as to constitute "public records."

Even if these communications are considered public records under FOIA and are not protected by ECPA, several exemptions may prevent disclosure (depending upon the particular communication). Among these are exemptions for:

- Information of a personal nature where public disclosure of the information would constitute a clearly unwarranted invasion of the individual's privacy, and the individual's interest in privacy clearly outweighs the public's right to know.
- Information contained in student records that would violate the Family Educational Rights and Privacy Act if released.
- Test questions and answers, scoring keys, and other examination instruments.
- Communications and notes within the University of an advisory nature to the extent that they cover other than purely factual information and are preliminary to a final University determination, policy, or action. (This particular exemption does not apply unless the public interest in encouraging frank communications between officials and employees of the University clearly outweighs the public interest in disclosure.)

III. Standards for Postmasters

Postmasters have specific responsibilities and access capabilities. Because of these special access capabilities they are expected to exercise special care in order to protect the privacy of the individuals whose electronic communications they handle. Note section I of this policy and also the overall policy regarding use of information technology resources (Standard Practice Guide #601.7, "Proper Use of Information Resources, Information Technology Resources, and Networks at the University of Michigan").

Postmasters at the University of Michigan shall maintain the following standards:

- Use machine headers and machine-generated messages in order to return undeliverable mail.
- Avoid reading message content to the greatest degree possible.
- Inform users of procedures for providing service, and assiduously attempt to respect privacy.
- Inform users and be straightforward if something goes wrong, in order to maintain trust.
- Keep confidential the content of any message that was inadvertently read in the course of redirecting undeliverable mail.
- Consult with users first if it seems necessary to go beyond machine-generated.
- Be informed about and follow University policy regarding privacy in electronic communication.

IV. Interpretive Guidelines and Procedures for System Administrators and Computing Service Managers

System administrators at the University of Michigan, in consultation with the relevant dean, director, or department chairperson, must determine where on the security versus service continuum (refer to section II, "Policy Interpretations") their particular mail system resides. They must inform their users of the tradeoffs between service and security that exist on their system. System administrators must maintain the level of mail security that is deliverable under conditions described in section III, "Standards for Postmasters." Users in individual departments may prefer that mail service be moved even closer to the secure end of this continuum. Therefore, there may ultimately be a need for several different options for users campus-wide. At a minimum, however, the guidelines for user information and mail privacy described in what follows, as well as section III above, must be met.

System administrators at U-M will need to take specific actions to ensure, to the greatest degree possible, that University policy is followed and that users are informed about the degree of privacy of their communications. The following list of information items will help users be as knowledgeable as possible about the systems that they use. It will also help system administrators manage the issues of electronic mail and privacy.

STANDARD PRACTICE GUIDE

THE UNIVERSITY OF MICHIGAN

NUMBER	601.11
DATE ISSUED:	12/1/93
PAGE	6 OF 6

SECTION: General University Policies

SUBJECT: Privacy of Electronic Mail and Computer Files at the University of Michigan

Provide information to users to answer the following questions:

- Is undeliverable mail discarded, examined for delivery clues, or automatically returned to sender?
- Is message content stripped from rejected or undeliverable mail?
- Are messages stored in clear text or encrypted while waiting to be delivered? How are they stored after delivery?
- What effect does file system backup have? (Is e-mail backed up? How long are backups retained? How often are backups made?)
- Where is the mail stored while waiting to be delivered and after delivery? How secure is that location?
- When I delete a message is it gone?
- Does the system make a copy of rejections? With text or without?
- If I go off campus, how long is my mail held for me? Are there limits on how much mail I can receive, store, have waiting?
- How long will my machine try to deliver outgoing mail before returning it as undeliverable?
- Is there a way my mail can be absolutely private?
- Should I send sensitive documents by e-mail?
- Can I encrypt mail?
- What kind of security features are available to me now? What is planned for the future, and when will that become available?

Until the technology catches up with the University community's desire for privacy, there are several recommended actions that a system administrator may wish to consider and/or take. They are listed in descending order from actions designed to protect privacy as much as possible to those ensuring the least degree of privacy:

- Use encryption software packages.
- Install a filter to keep text from view of postmasters or others.
- Require postmasters and others to adjust windows on their screens in order to exclude text.
- Train and expect those with special access privileges to "attention out" before the text of a message scrolls by.
- Set a standard of asking the user's permission prior to looking at text.
- Train and expect those with special access to use special self-restraint or to ignore the content of any private message/file.

This document represents current University of Michigan policy regarding the privacy of electronic communications and computer files. For further information regarding these issues, contact the Assistant for Policy Studies in the Information Technology Division, the University Information Officer, or the University General Counsel's Office.

Exhibit O-2

Paula -

Per my email dated 8/30/04.

kb.
4-2571

THE UNIVERSITY OF MICHIGAN

STANDARD PRACTICE GUIDE

Paul N. Courant
8/30/04

SECTION: General University Policies

Number: 601.11

Revised: 9/7/2004

SUBJECT: Privacy and the Need to Monitor and Access Records

Date Issued: 12/1/93

Attachment(s) 0

APPLIES TO: All Employees

ISSUED BY: Provost and Executive Vice President for Academic Affairs

I. Background

The University of Michigan respects the privacy of its employees and seeks to foster a climate free from arbitrary or capricious monitoring of employees and the *records*[1] they create, use, or control.

Nonetheless, the University must, at times, access *records* or monitor *record systems* that are under the control of its employees. Furthermore, because the University permits some latitude for employees to use University resources to conduct University business off-campus and to conduct personal matters at their work sites, *work-related records* and employees' *personal records* may be located in the same place.

This policy defines the rights, responsibilities, and expectations of the University and its employees regarding the conditions under which they may access *records* and monitor *record systems*.

II. Policy

There are many laws that govern the maintenance and disclosure of *records*. Federal and state laws, for example, require the University to:

- protect from unwarranted disclosure certain *records* of patients (HIPAA), students (FERPA), or library patrons (Michigan Library Privacy Act);
- disclose *records* (Freedom of Information Act, see http://www.umich.edu/~urel/foia.html, subpoenas, etc.); and/or
- monitor *record systems.*

Accordingly, the University of Michigan cannot guarantee the privacy of any *records*, including the *personal records*, of any University employee.

[1] Words that appear in *italics* are defined in section VI, Definitions.

This policy governs those circumstances in which the University, when not governed by external law, will monitor or access *records* and *record systems*.

Other than as authorized under the regulations of this policy, neither the University nor any employee acting on behalf of the University will access *records* or monitor the content of *record systems* located on University-controlled premises or University property, which includes but is not limited to University computers, networks, offices, and telephones.

III. Regulations

A. University Obligations

1. Standards for Accessing or Monitoring *Records*

As described below, the University has established general standards for accessing or monitoring all types of *records* (*business, faculty-owned scholarly*, and *personal*) or *record systems*, and additional standards for accessing or monitoring each type of *record*.

a. Standards that apply to all *business, faculty-owned scholarly,* and *personal records* or *record systems*

The University may access or monitor all *records (business, faculty-owned scholarly*, and *personal*) or *record systems* in the following circumstances:

1. When the University must monitor *record systems* to avert reasonably anticipated threats or hazards to those *record systems*. An example includes scanning to detect computer viruses. (This does not include an examination of the contents of *records* or *record systems.*); or

2. When the University is required by law to access, monitor, or disclose *records* or *record systems*.

b. Standards that apply to each type of *record (business, faculty-owned scholarly, and personal)*

1. *Business Records*

The University may access *business records* or monitor the *business record* content of *record systems* in the following circumstances:

- When the University has a *legitimate business need* to know or access the information contained in *business records,* and the employee who controls the *business records* or access to the *business records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access.

2. *Faculty-Owned Scholarly Records*

According to the 1940 Statement of Principles on Academic Freedom and Tenure, American Association of University Professors' Policy Documents & Reports (1995 ed.), "Institutions of higher education are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free expression."

Consistent with academic freedom and tradition, all University of Michigan faculty (including full-time, part-time, adjunct, and emeritus faculty) own and control instructional materials and scholarly works created at their own initiative with usual University resources. (For more information regarding ownership of works, see SPG section 601.03-2 "Ownership of Copyrighted Works Created at or in Affiliation with the University of Michigan.")

For the purposes of this policy the monitoring and access standards that apply to *faculty-owned scholarly records* (or *records* that are labeled as such) will also apply to *personal records.*

3. *Personal Records*

The University and its employees will not access or monitor the content of *personal records* (including *faculty-owned scholarly records*), or monitor the *personal records* (including *faculty-owned scholarly records*) content of *record systems*, except under the following circumstances:

a. When an employee who controls *faculty-owned scholarly* or *personal records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access and when it is necessary for the University to determine whether there are *business records* contained therein, the University will access such *records* only to the extent necessary; or

b. When there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly.

2. Preserving and Protecting *Records*

In circumstances where the University determines that there may be a specific risk to the integrity or security of *records*, the University may take measures to protect or preserve those *records*. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict access to a *record system*. The University may access or monitor preserved or protected *records* pursuant to Part III of this policy.

B. Employee Obligations

1. File Maintenance

a. *Work-Related Records*. Employees are responsible for organizing their *work-related records* so that they are accessible to those with a *legitimate business need* to know or access the information contained in them.

b. *Faculty-owned Scholarly* or *Personal Records*. While the University cannot provide an absolute guarantee as to the privacy of *faculty-owned scholarly* or *personal records*, employees should take reasonable measures to safeguard against inappropriate or inadvertent access to their *records*. Employees should mark as "private" or "personal" all *personal records*, or as "scholarship" or "research" all *faculty-owned scholarly records* maintained on University-controlled premises or property. Employees should maintain this information in an identifiable separate location (e.g. folder or file) from their *business records*.

2. Standards of Employee Conduct for Accessing or Monitoring *Records*

It is a violation of this policy for an employee to monitor *record systems* or access *records* beyond the standards established by Section III. A. of this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access *records*) and if the employee has accessed or monitored *records* or *record systems* for purposes other than the purposes for which the University has granted access.

IV. Sanctions

Violations of this policy will be considered misconduct on the part of the employee and will be subject to institutional sanctions up to and including termination of appointment.

Violations of this policy include:

1. An employee monitors *record systems* or accesses *records* beyond the standards established by Section III. A. of this policy.

2. The University has granted access to the employee (to monitor or access *records*) and the employee accesses or monitors *records* or *record systems* for purposes other than the purposes for which the University has granted access.

V. Employee Grievances

Employees who allege that the University has violated their rights as described in this policy may file a grievance under the appropriate University grievance procedure. Staff members should see Standard Practice Guide 201.08 "Grievance Procedures and Dispute Resolution" (http://spg.umich.edu/pdf/201.08.pdf) and faculty members should see the Faculty Handbook, Section 10.H "Formal Grievance Procedures" (http://www.provost.umich.edu/faculty/handbook/10/10.H.html); union members (faculty or staff) should refer to the grievance procedure in the applicable collective bargaining agreement.

VI. Definitions

A. Records

For purposes of this policy, a record is any document, file, computer program, database, image, recording, or other means of expressing fixed information that is created, received, used, or maintained within the scope of University business or employment at the University or that resides on University-controlled premises or property. Records are either *work-related* or *personal.*

B. Record Systems

Record systems are ways of storing, disseminating, or organizing *records*. They include, but are not limited to, computers, computing networks, telephones lines, voice mail, fax machines, filing cabinets, etc. which are University property or which are controlled by the University.

C. Work-Related Records

Work-related records are either *business records* or *scholarly records*.

D. Business Records

A business record is any *record* created, received, used, or maintained by an employee in the normal course of his or her professional responsibility or work for the University. This includes *records* relating to an employee's professional development, but does not include *faculty-owned scholarly records*. Examples of business records are drafts or final documents, including underlying or supporting documentation, of the following:

- □ budget reports;
- □ documents shared with or generated by third parties, such as purchase orders, bills for services or contracts with vendors;
- □ data sets that do not meet the definition of *faculty-owned scholarly records,* such as financial or enrollment data;
- □ feasibility studies or utilization analysis;
- □ attendance records, work schedules, or work orders;
- □ architectural drawings;

- ❑ correspondence or memoranda related to University business;
- ❑ course syllabi;
- ❑ student grades;
- ❑ meeting minutes;
- ❑ departmental web sites or e-mail groups; and
- ❑ committee reports.

E. Faculty-Owned Scholarly Records

Faculty-owned scholarly records are defined in SPG section 601.03-2 "Ownership of Copyrighted Works Created at or in Affiliation with the University of Michigan" as works that are created at the faculty member's own initiative with usual University resources. They include, but are not limited to *records* related to information gathering, knowledge production, methodology, distribution, handouts, reading lists, research, research plans, notes, charts, articles, presentations, books, scholarly commentary, consulting works, films, music, choreography, works of art, and all other *records* produced in the role of scholar, researcher, teacher, or faculty member. They do not include grades or course syllabi, nor do they include *records* produced using unusual University resources, commissioned works, or *records* created as a result of a faculty member's administrative appointment, or service to the University, such as committee work or serving as a hearing officer.

F. Personal Records

A personal record is a *record* that is created, received, used, or maintained by an employee for a purpose not related in any way to his or her work for the University.

G. Legitimate Business Need

A legitimate business need is any reason necessary to conduct the normal business of the University. A legitimate business need can be held only by a person who, based strictly on his or her job responsibilities, has a specific need to know the information accessed or monitored. The normal business of the University includes, but is not limited to:

- ❑ preparation of departmental budgets;
- ❑ ordering of materials, supplies, and equipment for the unit;
- ❑ activity related to providing service, such as food service, human resources, legal services, computer support services, etc.;
- ❑ strategic planning activity;

- ❑ planning, financing and construction of capital projects;
- ❑ preparation of work schedules;
- ❑ duties related to University committees; or
- ❑ audits of University finances, processes, and related activity.

Legitimate business need does *not* include access or monitoring the content of *records* or *record systems* in order to determine:

- ❑ whether a faculty or staff member is spending an excessive amount of work time on personal activities; or
- ❑ whether a faculty or staff member has committed misconduct, unless there is reasonable cause to believe that misconduct has been committed, *and* that University resources may have been used improperly.

Exhibit O-3

UNIVERSITY OF MICHIGAN

SPG U-M Standard Practice Guide

Privacy and the Need to Monitor and Access Records

601.11

I. Background

The University of Michigan respects the privacy of its employees and seeks to foster a climate free from arbitrary or capricious monitoring of employees and the *records*[1] they create, use, or control.

Nonetheless, the University must, at times, access *records* or monitor *record systems* that are under the control of its employees. Furthermore, because the University permits some latitude for employees to use University resources to conduct University business off-campus and to conduct personal matters at their work sites, *work-related records* and employees' *personal records* may be located in the same place.

This policy defines the rights, responsibilities, and expectations of the University and its employees regarding the conditions under which they may access *records* and monitor *record systems*.

II. Policy

There are many laws that govern the maintenance and disclosure of *records*. Federal and state laws, for example, require the University to:

- protect from unwarranted disclosure certain *records* of patients (HIPAA), students (FERPA), or library patrons (Michigan Library Privacy Act);
- disclose *records* (Freedom of Information Act, see http://www.umich.edu/~urel/foia.html, subpoenas, etc.); and/or
- monitor *record systems*.

Accordingly, the University of Michigan cannot guarantee the privacy of any *records*, including the *personal records*, of any University employee.

This policy governs those circumstances in which the University, when not governed by external law, will monitor or access *records* and *record systems*.

Other than as authorized under the regulations of this policy, neither the University nor any employee acting on behalf of the University will access *records* or monitor the content of *record systems* located on University-controlled premises or University property, which includes but is not limited to University computers, networks, offices, and telephones.

III. Regulations

A. University Obligations

1. Standards for Accessing or Monitoring Records

As described below, the University has established general standards for accessing or monitoring all types of *records* (*business*, *faculty-owned scholarly*, and *personal*) or *record systems*, and additional standards for accessing or monitoring each type of *record*.

a. Standards that apply to all *business*, *faculty-owned scholarly*, and *personal records* or *record systems*

The University may access or monitor all records (*business*, *faculty-owned scholarly*, and *personal*) or *record systems* in the following circumstances:

1. When the University must monitor *record systems* to avert reasonably anticipated threats or hazards to those *record systems*. An example includes scanning to detect computer viruses. (This does not include an examination of the contents of *records* or *record systems*.); or
2. When the University is required by law to access, monitor, or disclose *records* or *record systems*.

b. Standards that apply to each type of record (*business*, *faculty-owned scholarly*, and *personal*)

1. *Business Records*

The University may access *business records* or monitor the *business record* content of *record systems* in the following circumstances:

- When the University has a *legitimate business* need to know or access the information contained in *business records*, and the employee who controls the business records or access to the *business records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access.

2. *Faculty-Owned Scholarly Records*

According to the 1940 Statement of Principles on Academic Freedom and Tenure, American Association of University Professors' Policy Documents & Reports (1995 ed.), "Institutions of higher education are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free expression."

Consistent with academic freedom and tradition, all University of Michigan faculty (including full-time, part-time, adjunct, and emeritus faculty) own and control instructional materials and scholarly works created at their own initiative with usual University resources. (For more information regarding ownership of works, see SPG section 601.28 "Who Holds Copyright at or in Affiliation with the University of Michigan")

For the purposes of this policy the monitoring and access standards that apply to *faculty-owned scholarly* records (or records that are labeled as such) will also apply to *personal records*.

3. *Personal Records*

The University and its employees will not access or monitor the content of *personal records* (including *faculty-owned scholarly records*), or monitor the *personal records* (including *faculty-owned scholarly records*) content of *record systems*, except under the following circumstances:

a. When an employee who controls *faculty-owned scholarly* or *personal records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access and when it is necessary for the University to determine whether there are *business records* contained therein, the University will access such *records* only to the extent necessary; or

b. When there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly.

2. Preserving and Protecting *Records*

In circumstances where the University determines that there may be a specific risk to the integrity or security of *records*, the University may take measures to protect or preserve those *records*. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict access to a *record system*. The University may access or monitor preserved or protected *records* pursuant to Part III of this policy.

B. Employee Obligations

1. File Maintenance

a. *Work-Related Records*. Employees are responsible for organizing their *work-related records* so that they are accessible to those with a *legitimate business* need to know or access the information contained in them.

b. *Faculty-owned Scholarly* or *Personal Records*. While the University cannot provide an absolute guarantee as to the privacy of *faculty-owned scholarly* or *personal records*, employees should take reasonable measures to safeguard against inappropriate or inadvertent access to their *records*. Employees should mark as "private" or "personal" all *personal records*, or as "scholarship" or "research" all *faculty-owned scholarly records* maintained on University-controlled premises or property. Employees should maintain this information in an identifiable separate location (e.g. folder or file) from their *business records*.

2. Standards of Employee Conduct for Accessing or Monitoring *Records*

It is a violation of this policy for an employee to monitor *record systems* or access *records* beyond the standards established by Section III. A. of this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access *records*) and if the employee has accessed or monitored *records* or *record systems* for purposes other than the purposes for which the University has granted access.

IV. Sanctions

Violations of this policy will be considered misconduct on the part of the employee and will be subject to institutional sanctions up to and including termination of appointment.

Violations of this policy include:

1. An employee monitors *record systems* or accesses *records* beyond the standards established by Section III. A. of this policy.
2. The University has granted access to the employee (to monitor or access records) and the employee accesses or monitors *records* or *record systems* for purposes other than the purposes for which the University has granted access.

V. Employee Grievances

Employees who allege that the University has violated their rights as described in this policy may file a grievance under the appropriate University grievance procedure. Staff members should see Standard Practice Guide 201.08 "Grievance Procedures and Dispute Resolution" http://spg.umich.edu/pdf/201.08.pdf and faculty members should see the Faculty Handbook, Section 10.H "Formal Grievance Procedures" (http://www.provost.umich.edu/faculty/handbook/10/10.H.html); union members (faculty or staff) should refer to the grievance procedure in the applicable collective bargaining agreement.

VI. Definitions

A. Records

For purposes of this policy, a record is any document, file, computer program, database, image, recording, or other means of expressing fixed information that is created, received, used, or maintained within the scope of University business or employment at the University or that resides on University-controlled premises or property. Records are either *work-related* or *personal.*

B. Record Systems

Record systems are ways of storing, disseminating, or organizing *records*. They include, but are not limited to, computers, computing networks, telephones lines, voice mail, fax machines, filing cabinets, etc. which are University property or which are controlled by the University.

C. Work-Related Records

Work-related records are either *business records* or *scholarly records*.

D. Business Records

A business record is any *record* created, received, used, or maintained by an employee in the normal course of his or her professional responsibility or work for the University. This includes *records* relating to an employee's professional development, but does not include *faculty-owned scholarly records*. Examples of business records are drafts or final documents, including underlying or supporting documentation, of the following:

- budget reports;
- documents shared with or generated by third parties, such as purchase orders, bills for services or contracts with vendors;
- data sets that do not meet the definition of *faculty-owned scholarly records*, such as financial or enrollment data;
- feasibility studies or utilization analysis;
- attendance records, work schedules, or work orders;
- architectural drawings;
- correspondence or memoranda related to University business;
- course syllabi;
- student grades;

- meeting minutes;
- departmental web sites or e-mail groups; and
- committee reports.

E. Faculty-Owned Scholarly Records

Faculty-owned scholarly records are defined in SPG section 601.03 "Ownership of Copyrighted Works Created at or in Affiliation with the University of Michigan" as works that are created at the faculty member's own initiative with usual University resources. They include, but are not limited to *records* related to information gathering, knowledge production, methodology, distribution, handouts, reading lists, research, research plans, notes, charts, articles, presentations, books, scholarly commentary, consulting works, films, music, choreography, works of art, and all other *records* produced in the role of scholar, researcher, teacher, or faculty member. They do not include grades or course syllabi, nor do they include *records* produced using unusual University resources, commissioned works, or *records* created as a result of a faculty member's administrative appointment, or service to the University, such as committee work or serving as a hearing officer.

F. Personal Records

A personal record is a *record* that is created, received, used, or maintained by an employee for a purpose not related in any way to his or her work for the University.

G. Legitimate Business Need

A legitimate business need is any reason necessary to conduct the normal business of the University. A legitimate business need can be held only by a person who, based strictly on his or her job responsibilities, has a specific need to know the information accessed or monitored. The normal business of the University includes, but is not limited to:

- preparation of departmental budgets;
- ordering of materials, supplies, and equipment for the unit;
- activity related to providing service, such as food service, human resources, legal services, computer support services, etc.;
- strategic planning activity;
- planning, financing and construction of capital projects;
- preparation of work schedules;
- duties related to University committees; or
- audits of University finances, processes, and related activity.

Legitimate business need does **not** include access or monitoring the content of *records* or *record systems* in order to determine:

- whether a faculty or staff member is spending an excessive amount of work time on personal activities; or
- whether a faculty or staff member has committed misconduct, unless there is reasonable cause to believe that misconduct has been committed, *and* that University resources may have been used improperly.

[1] Words that appear in italics are defined in section VI, Definitions.

Attachment	Size
Printable PDF of SPG 601.11	43.52 KB

SPG number:
601.11

Date issued:
September 7, 2004

Applies to:
All Employees

Owner:
Office of the Provost and Executive Vice President for Academic Affairs

Related policies:
Grievance Procedure and Dispute Resolution

Related links:
Communications

Next review date:	Primary Contact:
September 7, 2008	Office of the Provost and Executive Vice President for Academic Affairs

Hard copies of this document are considered uncontrolled. If you have a printed version, please refer to the University SPG website (spg.umich.edu) for the official, most recent version.